

CLAIMS

What is claimed is:

1. A method for allowing an Internet or intranet browser user to transfer directly

to a domain that is participating in an e-community without repetitious and

5 redundant authentication actions, said e-community comprising a plurality

of affiliated domain servers, said user being properly registered and

authenticated to a home domain server within said e-community,

said method comprising the steps of:

enrolling said user at an affiliated domain through exchange

10 of a home domain identity cookie with enrollment request and an affiliated

domain identity cookie with enrollment response success indicator between

said home domain server and an affiliated domain server;

vouching for the identity of the user through exchange of a vouch-for

request and vouch-for response between said home domain server and an

15 affiliated domain server;

building a local session at said affiliated domain for said user using

said protected resource responsive to receipt of said vouch-for response; and

transmitting an e-community cookie from said affiliated domain server

to said browser recording successful authentication of said user into said

20 affiliated domain.

2. The method as set forth in Claim 1 wherein said step of enrolling the user at

an affiliated domain comprises the steps of:

transmitting a home domain identity cookie and enrollment request by said home domain server to a user's browser where it may be stored; redirecting said enrollment request to an affiliated domain server; transmitting an affiliated domain identity cookie with an enrollment 5 response including an enrollment success indicator from said affiliated domain server to said user's browser; redirecting said enrollment response with enrollment success indicator to said home domain server where it may be stored; updating a set of user information at said home domain to record 10 enrollment success at said affiliated domain server such that there is a server-maintained persistent record of the user's enrollment; and modifying said home domain identity cookie to record enrollment success at said affiliated domain server such that there is a user-maintained 15 persistent record of the user's enrollment so that the user may access and use resources associated with the affiliated domain server.

3. The method as set forth Claim 2 wherein said step of redirecting said enrollment request comprises performing a hyper text transfer protocol redirection operation.

4. The method as set forth Claim 2 wherein said step of redirecting said 20 enrollment success indicator to said home domain server comprises performing a hyper text transfer protocol redirection operation.

5. The method as set forth Claim 2 wherein said step of modifying said home

domain identity cookie to record enrollment success at said affiliated domain server comprises modifying extensible data in the home domain identity cookie to include a symbol indicating successful enrollment at said affiliated domain server.

5 6. The method as set forth in Claim 1 wherein said step of vouching for the identity of the user comprises the steps of:

transferring said affiliated domain identity cookie with access request for a protected resource from said user's browser to said affiliated domain server;

10 extracting the user's home domain identity from the affiliated domain identity cookie in order to determine where to send a vouch-for request;

sending a vouch-for request from said affiliated domain server to said home domain server via the user's browser using redirection; and

15 returning a vouch-for response to said affiliated domain server from said home domain server via the user's browser using redirection.

7. The method as set forth in Claim 6 wherein said step of sending a vouch-for request from said affiliated domain server to said home domain comprises the step of determining the user's home domain server by evaluation of the user's affiliated domain identity cookie.

20 8. The method as set forth in Claim 6 wherein said step of sending a vouch-for request from said affiliated domain server to said home domain server comprises performing a hyper text transfer protocol redirection operation.

9. The method as set forth in Claim 6 wherein said step of returning a vouch-for response to said affiliated domain server from said home domain server comprises performing a hyper text transfer protocol redirection operation.

10. A computer readable medium encoded with software for allowing an Internet or intranet browser user to transfer directly to a domain that is participating in an e-community without repetitious and redundant authentication actions, said e-community comprising a plurality of affiliated domain servers, said user being properly registered and authenticated to a home domain server within said e-community, said software causing a processor to perform the steps of:

10 enrolling said user at an affiliated domain through exchange of a home domain identity cookie with enrollment request and an affiliated domain identity cookie with enrollment response success indicator between said home domain server and an affiliated domain server;

15 vouching for the identity of the user through exchange of a vouch-for request and vouch-for response between said home domain server and an affiliated domain server;

building a local session at said affiliated domain for said user using said protected resource responsive to receipt of said vouch-for response; and

transmitting an e-community cookie from said affiliated domain server to said browser recording successful authentication of said user into said affiliated domain.

20 11. The computer readable medium as set forth in Claim 10 wherein said software

for enrolling the user at an affiliated domain comprises software for performing the steps of:

transmitting a home domain identity cookie and enrollment request by said home domain server to a user's browser where it may be stored;

5 redirecting said enrollment request to an affiliated domain server;

transmitting an affiliated domain identity cookie with an enrollment response including an enrollment success indicator from said affiliated domain server to said user's browser;

10 redirecting said enrollment response with enrollment success indicator to said home domain server where it may be stored;

updating a set of user information at said home domain to record enrollment success at said affiliated domain server such that there is a server-maintained persistent record of the user's enrollment; and

15 modifying said home domain identity cookie to record enrollment success at said affiliated domain server such that there is a user-maintained persistent record of the user's enrollment so that the user may access and use resources associated with the affiliated domain server.

12. The computer readable medium as set forth in Claim 11 wherein said software for redirecting said enrollment request comprises software for performing a hyper text transfer protocol redirection operation.

20

13. The computer readable medium as set forth in Claim 11 wherein said software for redirecting said enrollment success indicator to said home domain server

comprises software for performing a hyper text transfer protocol redirection operation.

14. The computer readable medium as set forth in Claim 11 wherein said software for modifying said home domain identity cookie to record enrollment success at said affiliated domain server comprises software for modifying extensible data in the home domain identity cookie to include a symbol indicating successful enrollment at said affiliated domain server.

15. The computer readable medium as set forth in Claim 10 wherein said software
for vouching for the identity of the user comprises software for performing the
10 steps of:

transferring said affiliated domain identity cookie with access request for a protected resource from said user's browser to said affiliated domain server;

15 extracting the user's home domain identity from the affiliated domain
identity cookie in order to determine where to send a vouch-for request;

sending a vouch-for request from said affiliated domain server to said home domain server via the user's browser using redirection; and

returning a vouch-for response to said affiliated domain server from said home domain server via the user's browser using redirection.

20 16. The computer readable medium as set forth in Claim 15 wherein said software
for sending a vouch-for request from said affiliated domain server to said home
domain comprises software for determining the user's affiliated domain server

by evaluation of the user's home domain identity cookie.

17. The computer readable medium as set forth in Claim 15 wherein said software for sending a vouch-for request from said affiliated domain server to said home domain server comprises software for performing a hyper text transfer protocol redirection operation.

5

18. The computer readable medium as set forth in Claim 15 wherein said software for returning a vouch-for response to said affiliated domain server from said home domain server comprises software for performing a hyper text transfer protocol redirection operation.

10 19. A system for e-community enrollment by an Internet or intranet user using cross-domain single-sign-on to a domain that is participating in an e-community without repetitious and redundant authentication actions, said e-community comprising a plurality of affiliated domain servers, said user being properly registered and authenticated to a home domain server within said e-community, said system comprising:

15

 a home domain identity cookie accompanying an enrollment request receivable by an affiliated domain server;

 an affiliated domain identity cookie accompanying an enrollment response success indicator receivable by said home domain server;

20

 a vouch-for request receivable by a home domain server; and

 a vouch-for response receivable by said affiliated domain server; and

 an e-community cookie receivable by said browser to record successful

authentication of said user into said affiliated domain for the duration of the user's session.

20. The system as set forth in Claim 19 further comprising:

an enrollment request redirector for redirecting said enrollment request from said home domain server to an affiliated domain server via said browser;

an enrollment response redirector for redirecting said enrollment response with enrollment success indicator to said home domain server from said affiliated domain server via said browser;

10 a user information manager operable by said home domain adapted to record enrollment success at said affiliated domain server such that there is a server-maintained persistent record of the user's enrollment; and

a home domain identity cookie modifier adapted to record enrollment success at said affiliated domain server such that there is a client-maintained persistent record of the user's enrollment so that the user may access and use resources associated with the affiliated domain server.

15

21. The system as set forth Claim 20 wherein said enrollment request redirector comprises a hyper text transfer protocol command.

22. The system as set forth Claim 20 wherein said enrollment response redirector comprises a hyper text transfer protocol redirection command.

20

23. The system as set forth Claim 20 wherein said home domain identity cookie modifier is adapted to modify extensible data in the home domain identity

cookie to include a symbol indicating successful enrollment at said affiliated domain server.

24. The system as set forth in Claim 19 further comprising an affiliated domain identity cookie evaluator for extracting the user's home domain identity from said affiliated domain identity cookie in order to determine where to send a vouch-for request.

5